UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/888,838	06/25/2001	Vladimir Castro Alves	MORPH1160	4398

29585 7590 03/16/2005

DLA PIPER RUDNICK GRAY CARY US LLP
153 TOWNSEND STREET
SUITE 800
SAN FRANCISCO, CA 94107-1907

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/888,838	ALVES ET AL.	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 12/27/02
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-10, 19-25, 30-36, 41 are rejected under 35 U.S.C. 102(e) as being anticipated by Jones, U.S. Patent No. 6,088,800. Referring to claims 1, 19, 21, 22, 31-33, 41, Jones discloses an encryption processor with shared memory wherein the electronic encryption device comprises an array of processing elements (Col. 3, lines 46-48), which meets the limitation of a portion of an array of processing elements for performing a block cipher routine. Each processing element comprises an instruction memory for storing a round of an encryption algorithm, the round comprising a sequence of instructions (Col. 3, lines 48-51), which meets the limitation of the processing elements being independently reconfigurable. Data enters the encryption device

through an input stage (Fig. 2, 40 & Col. 6, lines 3-4), which meets the limitation of receiving an input data block at an array of independently reconfigurable processing elements. Each processing element of the array implements one of the rounds and transfers results to successive processing elements such that the array of processing elements implements successive rounds of the encryption algorithm in a processing element pipeline (Col. 3, lines 51-59), which meets the limitation of executing the block cipher routine on data blocks received at the configured portion of the array of processing elements, outputting encrypted data from the configured portion of the array of processing elements, wherein the encrypted data is encrypted according to the block cipher routine. Figure 2 shows a global memory that is shared between the processing elements to perform the encryption processes (Col. 7, lines 25-38), which meets the limitation of a context memory for storing one or more context instructions for performing a block cipher routine.

Referring to claims 2, the limitation of the activation signal is meet by the sequence of instructions that each processing element receives on a round to round basis (Col. 3, lines 48-51).

Referring to claims 3, 5, Jones discloses using multiple secret keys during the block ciphering process (Col. 1, line 62 – Col. 2, line 4), which meets the limitation of configuring a portion of the array of reconfigurable processing elements further includes loading a plurality of subkeys into the active processing elements.

Referring to claims 2, 4, 7-9, 20, 23, 25, Jones discloses that the encryption chip and processing elements can perform encryption, decryption, and message digest functions (Col. 5, line 64 – Col. 6, line 2), which meets the limitation of executing the block cipher routine includes executing one of the plurality of subfuctions according to the context instruction, data blocks are encrypted, and wherein the method further comprises outputting decrypted data from the

configured portion of the array of processing elements, wherein the decrypted data is decrypted according to the block cipher routine, the block cipher routine is a decryption routine.

Referring to claims 10, 30, 34-36, Jones discloses the array of processing elements includes an M-row by N-column number of processing elements, wherein M is equal to n and N is equal to 1 (Fig. 2).

Referring to claim 24, Jones discloses that the secret keys used in the encryption processor are generated (Col. 2, lines 1-2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 11-18, 26-29, 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones, U.S. Patent No. 6,088,800, in view of Sorimachi, US 2002/0181709. Referring to claims 11-17, 26-29, 37-40, Jones discloses an encryption processor with shared memory wherein the electronic encryption device comprises an array of processing elements (Col. 3, lines

46-48), which meets the limitation of a portion of an array of processing elements for performing a block cipher routine. Each processing element comprises an instruction memory for storing a round of an encryption algorithm, the round comprising a sequence of instructions (Col. 3, lines 48-51), which meets the limitation of the processing elements being independently reconfigurable. Data enters the encryption device through an input stage (Fig. 2, 40 & Col. 6, lines 3-4), which meets the limitation of receiving an input data block at an array of independently reconfigurable processing elements. Each processing element of the array implements one of the rounds and transfers results to successive processing elements such that the array of processing elements implements successive rounds of the encryption algorithm in a processing element pipeline (Col. 3, lines 51-59), which meets the limitation of executing the block cipher routine on data blocks received at the configured portion of the array of processing elements. Jones discloses using DES, RC5, and IDEA encryption algorithms (Col. 5, lines 49-51), but does not disclose using the Kasumi block cipher algorithm. Sorimachi discloses an encryption system wherein the block cipher algorithm used is the Kasumi algorithm ([0372]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the encryption processor of Jones to use the Kasumi block cipher algorithm because Sorimachi discloses that the Kasumi algorithm is an alternative algorithm to DES ([0369]-[0372]).

Referring to claim 18, Jones discloses that the data blocks are 64-bit data blocks (Col. 15, line 10).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100